

NASM



National Attack Surface Management

National cyber situational awareness from technical intelligence

For cyber agencies, public authorities, defense and intelligence. Supervise public and private entities, critical infrastructure and strategic supply chains.



Public and private entities, critical infrastructure and shared digital dependencies



Non-intrusive supervision

Assess available intelligence near real time, without entity participation, agents, credentials or internal access.



Systemic risk visibility

Reveal shared vulnerabilities and provider dependencies through national, sector and regional views.



Actionable intelligence

Link priorities to entities, assets and threat context. Use alerts and reports to guide analyst action.

From aggregate risk to technical evidence

Start with a national, sector or regional view, then drill down to the organizations and assets behind each risk signal. Compare CVE prevalence, cloud and technology concentration, supplier dependencies and exposure trends. Geographical and jurisdictional views help identify infrastructure dependencies that warrant review against digital-sovereignty policies. Use comparable KPIs and technical findings to prioritize supervision, remediation campaigns and national resilience planning.

Operational intelligence

Connect national risk priorities to technical evidence. Review individual entities and aggregate exposure for institutional analysis, supervision and planning.

Entity-level evidence

Inspect domains, IPs, services and technologies per entity. Review asset-linked CVE context, configuration indicators, exposed credentials and observable OT/IoT.

Vulnerability concentration

Identify shared CVEs and vulnerable technologies across entities and sectors. Prioritize pervasive exposures for coordinated national remediation.

Geography & jurisdictions

Review infrastructure locations and provider geography against digital-sovereignty policies. Flag cross-border dependencies for technical or institutional review.

National & sector views

Compare scores, CVE prevalence and exposure trends by nation, sector, region or custom cohort. Drill down to entities and assets. Track resilience KPIs.

Provider & supply-chain risk

Map cloud, hosting and technology providers, critical suppliers and observable fourth parties. Identify shared dependencies and provider concentration.

Threat-actor relevance

Correlate CVEs with known exploitation, MITRE ATT&CK techniques and threat actors. Prioritize by exploitation history, targeted sectors and national context.

Sovereignty & mission customization

Dedicated cloud or optional full on-premise

Select cloud delivery or optional full on-premise on customer-controlled infrastructure when confidentiality and operational autonomy are essential.



Control and confidentiality

With full on-premise, the customer controls data, targets, users and access. Coinnect has no ordinary visibility into monitored entities. Support access requires customer authorization.

Customization & assurance

Customize risk models, taxonomies, KPIs, dashboards and workflows. Scope APIs, integrations and white-label interfaces for complex programs. Controlled source-code access supports audit under agreed terms.